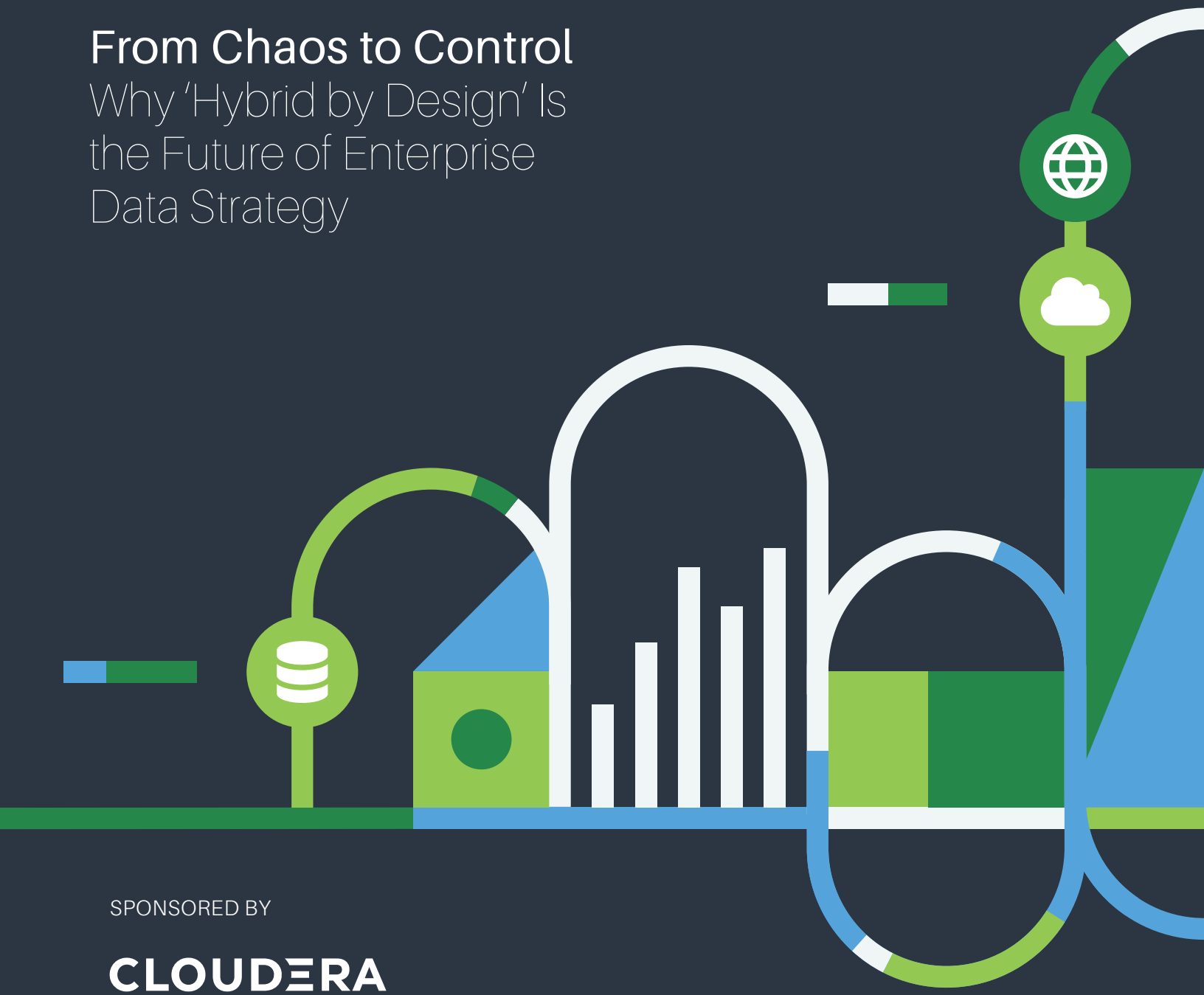
TechnologyAdvice

APRIL 2026

INDUSTRY TREND REPORT

From Chaos to Control

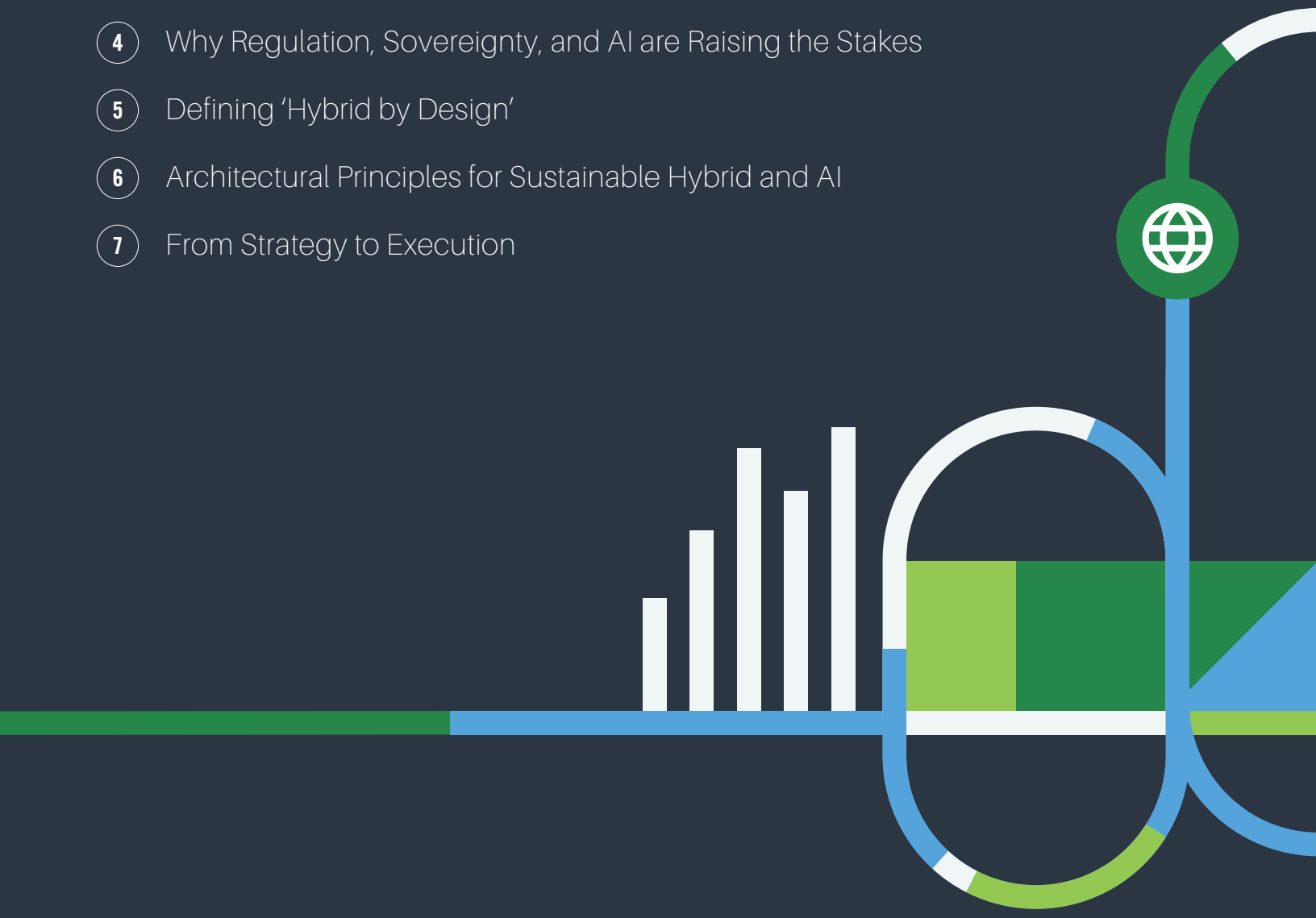
Why 'Hybrid by Design' Is the Future of Enterprise Data Strategy



SPONSORED BY

CLOUDERA

CONTENTS



From Chaos to Control: Why 'Hybrid by Design' Is the Future of Enterprise Data Strategy

FOCUS

Hybrid cloud was supposed to be a strategy. For many enterprises, it became an outcome. Over years of tactical cloud migrations, compliance mandates, M&A activity, and AI experimentation, organizations have unintentionally built fragmented hybrid environments that increase cost, complexity, and risk. This report explores the shift from "hybrid by accident" to "hybrid by design," outlining the architectural principles, governance models, and platform capabilities required to create resilient, compliant, AI-ready data ecosystems. It positions Cloudera as the strategic guide for enterprises ready to bring intentionality, control, and innovation to their hybrid and multi-cloud environments.

> "I define 'hybrid by accident' as the unintentional sprawl of fragmented data ecosystems across distributed environments. While hybrid cloud was originally intended to be a cohesive strategy, for many organizations it simply became a chaotic outcome. Instead of driving business value, organizations waste significant budget trying to wire disconnected systems together while battling highly unpredictable operational costs.
>
> **SERGIO GAGO HUERTA**
> CHIEF TECHNOLOGY OFFICER, CLOUDERA

THE RISE OF HYBRID BY ACCIDENT

Hybrid cloud was once framed as a deliberate enterprise strategy. The goal was to combine the flexibility of public cloud services with the control and performance of on-premises infrastructure. In practice, many organizations did not arrive at hybrid architecture through coordinated planning. Instead, hybrid environments emerged gradually as companies responded to immediate operational needs, regulatory requirements, and new technology initiatives.

Over the past decade, several common patterns have contributed to this shift. Cloud-first initiatives encouraged rapid migration of individual applications. Business units independently adopted software-as-a-service tools. Compliance mandates required certain datasets to remain in specific jurisdictions or within private infrastructure. Mergers and acquisitions introduced additional systems and data platforms that were never fully integrated. At the same time, organizations launched artificial intelligence pilots and analytics projects in multiple environments to accelerate experimentation.

These incremental decisions often occurred in isolation. Each decision solved a short-term problem, but collectively they produced complex hybrid environments with multiple clouds, data centers, and edge locations operating without consistent architectural oversight.

The operational consequences of this unplanned hybrid expansion are significant. Data becomes distributed across multiple environments with limited visibility into how it is accessed or governed. Teams create duplicate pipelines and analytics workflows to compensate for disconnected systems, while inconsistent governance and security policies increase compliance risk. At the same time, fragmented workloads make cost management difficult, leading to redundant services, unnecessary data movement, and unpredictable operational spending.

For many enterprises, the challenge is not whether hybrid infrastructure exists. The challenge is that hybrid environments evolved without a unified architectural model. As a result, organizations now operate highly distributed data ecosystems that require a more intentional strategy to restore visibility, governance, and operational control.

WHY REGULATION, SOVEREIGNTY, AND AI ARE RAISING THE STAKES

Regulatory pressure and governance expectations are rising as enterprises push AI into production, and the lack of a unified hybrid operating model is now creating measurable compliance, cost, and execution risk. As data estates expand across public cloud, on-premises infrastructure, and the edge, organizations are under greater scrutiny to prove control over where data resides and how it is accessed.

61%

of organizations are now seeking sovereign technology due to geopolitical tensions and compliance risks

Data governance now sits at the center of this challenge. Organizations need consistent visibility into sensitive data location, access, and use across environments. When governance is fragmented, it becomes harder to enforce policies consistently, validate lineage, and demonstrate compliance.

Gago Huerta explains why sovereignty and compliance requirements are forcing infrastructure decisions:

"On the regulatory front, intensifying data sovereignty laws, cross-border data restrictions, and sector-specific privacy mandates demand absolute control over where information resides. In fact, recent surveys show that 61% of organizations are now seeking sovereign technology due to geopolitical tensions and compliance risks."

AI is placing additional pressure on hybrid environments. Governance requirements become more complex as AI systems rely on trusted data inputs across distributed infrastructure. At the same time, the economics of operating AI at scale are influencing where workloads can run sustainably.

85-90%

of AI spend is consumed by inference & operational overhead as enterprises move generative AI into production

Gago Huerta notes that the economics of AI in production are forcing enterprises to rethink where workloads run.

"Compounding these compliance hurdles is the massive business pressure of the 'inference economics wake-up call'. As enterprises move generative AI into production, they are finding that 85-90% of their AI spend is consumed by inference and operational overhead. Attempting to run these workloads exclusively in the public cloud is financially unsustainable, as private AI can be nearly three times cheaper at enterprise scale."

For many enterprises, these combined pressures make reactive hybrid management unsustainable. Hybrid infrastructure is no longer just an infrastructure strategy. Resilience, compliance, and innovation increasingly depend on consistent governance and operating models across every environment where data is stored and processed. It is a control model that determines how organizations maintain compliance, protect sensitive data, and ensure that analytics and AI initiatives operate on trusted information.

DEFINING 'HYBRID BY DESIGN'

To respond to these pressures, enterprises are increasingly moving from reactive hybrid management to a deliberate operating model for data and AI. "Hybrid by design" represents an intentional operating model to run data platforms, analytics workloads, and AI systems across public cloud, data centers, and the edge with open standards, workload portability, and centralized governance.

At its core, intentional hybrid design prioritizes operational flexibility. Organizations gain the ability to decide where workloads should run based on business requirements such as performance, cost efficiency, resilience, locality, or sustainability goals.

Workload portability plays a central role in enabling this model. When applications and analytics workloads can run consistently across environments, enterprises can place compute resources where they are most effective while maintaining access to governed data. This approach reduces unnecessary data movement and allows organizations to optimize infrastructure usage without compromising compliance or performance.

Open standards support this flexibility by preventing dependence on proprietary data formats or isolated ecosystems. When data platforms rely on open technologies and interoperable architectures, organizations retain the freedom to evolve their infrastructure as business needs change. This reduces the risk of vendor lock-in and allows enterprises to respond more quickly to new regulatory, operational, or technological requirements.

The result is a hybrid environment that operates as a unified system rather than a collection of disconnected platforms. By designing hybrid architecture intentionally, enterprises gain the control and transparency required to support modern analytics and AI while maintaining governance across every location where data exists.

> Open standards and workload portability act as an enterprise's primary insurance policy against vendor lock-in and unpredictable cloud economics. In a landscape where hyperscalers can unilaterally alter pricing models or deprecate services, organizations tied to proprietary data formats and isolated compute engines lose their negotiating power and strategic agility.

SERGIO GAGO HUERTA EXPLAINS, PORTABILITY HAS BECOME A STRATEGIC SAFEGUARD AGAINST VENDOR LOCK-IN AND UNPREDICTABLE CLOUD ECONOMICS.

ARCHITECTURAL PRINCIPLES FOR SUSTAINABLE HYBRID AND AI

Achieving control and transparency across hybrid environments requires more than architectural intent. It requires a consistent set of principles that allow data, analytics, and AI workloads to run reliably across public cloud, data centers, and the edge.

Open ecosystems and standards

Open technologies provide the foundation for long-term flexibility. When data platforms rely on open table formats and interoperable tools, organizations avoid becoming locked into proprietary infrastructure. This approach ensures that enterprises maintain control over their data and can evolve their technology stack without being constrained by a single vendor ecosystem.

Workload portability

Rather than moving large volumes of data between platforms, organizations can bring workloads to where the data already resides. This reduces infrastructure cost, limits unnecessary data movement, and allows enterprises to optimize performance and compliance requirements across environments.

Unified governance and security

Governance must operate consistently across the entire hybrid estate. Applying a unified governance model ensures that security policies, access controls, and data lineage remain attached to the data regardless of where it resides. This consistency reduces compliance risk and supports trusted analytics and AI outcomes.

Gago Huerta also highlights the importance of unified governance in distributed environments.

"A unified governance model solves this by applying a single, consistent security policy across the entire hybrid estate. This approach ensures that access controls and data lineage stay firmly attached to the data, regardless of where it physically lives or moves. It also makes it much easier to prove strict compliance to regulators during an audit."

Real time data and AI operationalization

Modern analytics and AI applications increasingly rely on real-time and streaming data. Hybrid architectures must support data in motion as well as data at rest so organizations can generate insights and predictions as events occur. A unified architecture also enables teams to operationalize AI from development through production while maintaining governance across all environments.

Together, these principles reduce operational complexity, lower total cost of ownership, and enable faster deployment of analytics and AI workloads across environments.

FROM STRATEGY TO EXECUTION

Recognizing the need for intentional hybrid architecture is only the first step. The real challenge for enterprise leaders is translating strategy into an operational model that provides consistent governance, portability, and visibility across all environments where data exists.

Organizations must first assess where data resides across clouds, data centers, and edge deployments while evaluating the operational cost of moving and managing that data. This process often reveals duplicated pipelines, isolated data silos, and fragmented governance policies. With this visibility established, enterprises can standardize on open formats and portable workloads so analytics and AI services can run consistently across environments.

Governance must also be unified across the entire hybrid estate. Applying consistent access controls, lineage tracking, and security policies ensures that data remains trusted and compliant regardless of where it resides. With a unified governance model in place, organizations can provide reliable data access to analytics and AI systems while reducing operational risk.

Cloudera enables this transition by delivering a unified data and AI platform that allows organizations to run analytics and AI workloads wherever their data lives across cloud environments, data centers, and the edge. This architecture connects distributed data while maintaining consistent governance and security, enabling enterprises to operationalize AI without forcing large scale data movement.

Cloudera helps organizations unify their data estate, simplify hybrid operations, and bring AI directly to trusted data sources.

By providing a consistent cloud experience across environments, Cloudera helps organizations unify their data estate, simplify hybrid operations, and bring AI directly to trusted data sources. This approach allows enterprises to accelerate innovation while maintaining the control and compliance required in modern data ecosystems.